AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

INFORMATION ASSOCIATED WITH (937) 238-1132 AND (704) 497-3706 THAT IS STORED AT PREMISES CONROLLED BY AT&T WIRELESS

Case No. 3:20 mj 026

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
See Attachment C	

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Robert M. Buzzard
Applicant's signature

SA Robert M. Buzzard, FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 1-13-20

Sharon L. Ovington
Judge's signature

City and state: Dayton, Ohio

Sharon L. Ovington, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH (937) 238-1132 and (704) 497-3706 THAT IS STORED AT PREMISES CONROLLED BY AT&T WIRELESS	Case No. _____ **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Robert M. Buzzard, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises owned, maintained, controlled, or operated by AT&T Wireless, a wireless provider headquartered at 11760 US Highway 1, Ste. 600, North Palm Beach, FL 33408. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require **AT&T Wireless** to disclose to the government records and other information in its possession pertaining to the subscriber or customer associated with the accounts, including the contents of communications.

2. I am a Special Agent with the Federal Bureau of Investigations (FBI), and have been so employed since January of 2002. I am currently assigned to the Cincinnati Division, Dayton Resident Agency. As such, I am charged with investigating crimes against the United States of America, including but not limited to violations of Title 18 and Title 21 of the United States Code. I have received training in drug trafficking investigations and participated in

numerous narcotics-related investigations (ultimately leading to successful prosecution) that involved surveillance, the execution of search warrants, gathering evidence of money laundering, interviewing suspected drug traffickers, and supervising the activities of informants who provided information and assistance which resulted in the seizure of narcotics. I am familiar with federal drug laws, and am aware that it is a violation of Title 21, U.S.C., Sections 841(a)(1) and 846 to distribute and possess with intent to distribute controlled substances, as well as to conspire to do the same. I am also aware through my training and experience that drug traffickers commonly use cellular telephones and electronic devices to facilitate their drug trafficking activities/crimes.

3. Along with other agents, officers, and law enforcement officials from the DEA, ATF, and Dayton Police Department, I am currently involved in the investigation of drug trafficking and firearms offenses committed by Nathan GODDARD, Cahke CORTNER, Lionel COMBS III, and Courtney ALLEN—including violations of: 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances; 21 U.S.C. § 843(b) (use of a telephone communication facility to facilitate a drug trafficking crime); 21 U.S.C. § 846 (conspiracy to possess with intent to distribute controlled substances); 21 U.S.C. § 856(maintaining a drug premises); and 18 U.S.C. § 924(c) (use and carrying of a firearm during and in relation to a drug trafficking crime (hereinafter and collectively "Subject Offenses"). I have personally participated in this investigation and have spoken to, as well as received information from, other agents and investigators participating in this matter. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of the SUBJECT OFFENSES have been committed by GODDARD, COMBS, and CORTNER. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

7. Between mid-July and late October 2019, members of the DEA Dayton Resident Office conducted an investigation into a Dayton, Ohio based fentanyl trafficking organization. During that investigation, investigators developed a Cooperating Defendant (hereinafter referred to as CD). CD provided information to members of the DEA investigative team for possible consideration in an on-going drug trafficking investigation.

8. During subsequent interviews, CD identified Nathan GODDARD as CD's source of supply for illegal narcotics. CD estimated that he/she obtained approximately one pound of marijuana from GODDARD on or about November 3, 2019 inside a residence at 1454 Ruskin Rd., Dayton, Ohio. During that transaction, CD also observed approximately ten kilograms of suspected drugs present in the basement of the residence. GODDARD informed CD the suspected drugs were fentanyl. On November 4, 2019, DEA investigators monitored a cellular telephone call between CD and GODDARD. CD called GODDARD at cellular telephone number (704) 497-3706. During the conversation, CD and GODDARD discussed the prior purchase of marijuana on November 3, 2019 and GODDARD showing CD the kilograms of suspected fentanyl. CD asked GODDARD for the purchase price for one kilogram of fentanyl and GODDARD indicated $60,000. CD and GODDARD agreed to communicate at a later time to arrange for the purchase of fentanyl.

9. CD further explained to investigators there were two additional individuals inside the residence at 1454 Ruskin Rd. with GODDARD when the drug transaction occurred on November 3, 2019. The two individuals were later identified by the investigative team as Lionel Combs III and Cahke CORTNER. CD explained COMBS and CORTNER witnessed the marijuana transaction on November 3, 2019 and reported the kilograms of suspected fentanyl were laying out in the open for everyone in the basement to see (including COMBS and CORTNER). In addition, CD observed CORTNER and GODDARD in possession of similar firearms during and in relation to the narcotics transaction. CD described CORTNER appeared to be acting as an enforcer or body guard for GODDARD during the marijuana transaction.

10. On November 4, 2019, DEA Special Agent Charles Vill obtained a search warrant for the residence at 1454 Ruskin Rd., Dayton, Ohio authorized by U.S. Magistrate Judge Sharon L. Ovington, Southern District of Ohio. The search warrant authorized the seizure of contraband (to include illegal narcotics), U.S. currency, firearms/ammunition, electronic devices (to include cellular telephones and computers), and other items associated with drug trafficking activities.

11. At approximately 6:50 p.m., on November 4, 2019, members of the DEA investigative team executed the federal search warrant at 1454 Ruskin Rd. Upon lawful entry into the residence, DEA Task Force Officer (TFO) Jorge Del Rio was shot in the face by GODDARD as TFO Del Rio descended down a stairway into a basement. Following the shooting, GODDARD, CORTNER, COMBS, and Courtney ALLEN were detained by DEA officers in the basement.

12. During a subsequent search of the residence, law enforcement officers located and seized pounds of marijuana, more than six kilograms of cocaine, more than four kilograms of fentanyl, over $40,000 in U.S. currency, the firearm GODDARD used to shoot TFO Del Rio, a similar firearm possessed by CORTNER at the time of the search warrant, and a third firearm from the basement. Additionally, law enforcement officers located and seized fourteen cellular telephones.

13. One of those cellular telephones was an Apple iPhone, Model A1661, FCC ID: BCG-E3087A, IC:579C-E3087A, with an identified telephone number of 704-497-3706. The cellular phone was located and seized from the basement. Another cellular telephone was a Samsung Galaxy Note8, Serial Number: R38JA0LTZSB, IMEI: 35850208374203, with an

identified telephone number of (937) 238-1132. This cellular phone was also located and seized from the basement.

14. Based on my training and experience, I know the amount of the narcotics seized from the residence is indicative of a large-scale drug trafficking operation. I also know that, given the amount of drugs found at the location and indicia of drug trafficking throughout the house – including, for instance, a digital scale and cash in the upstairs of the residence, I believe that the men detained at the Ruskin residence were using this location as a drug premises. I also know that COMBS rented the Ruskin residence; in a post-Miranda interview, COMBS confirmed that he knew GODDARD was storing large quantities of marijuana and money at the residence.

15. I also believe that, given the amount of drugs seized from the residence, the men were not first time participants in the drug trade. (Indeed, GODDARD, has a prior federal conviction for drug trafficking). Based on my training and experience, I know that if often takes an extended period of time for individuals to gain trust from sources of supply to obtain that quantity of narcotics. (The drugs seized had street values in the hundreds of thousands of dollars). In short, based on my training and experience, this was not an isolated incident; rather, the men likely had been trafficking drugs for months prior to this incident.

16. Based on training and experience, your affiant knows that drug traffickers frequently use wireless/cellular telephones to carry out their activities. For instance, as described above, the CD communicated with GODDARD via cellular telephone. Drug dealers use cellular telephones to communicate with customers, their associates and their suppliers. It is often common for drug traffickers to have multiple telephones because certain phones may be used

only for certain purposes. For instance, a trafficker may use one telephone just to speak to his supplier, while using a different phone to speak only to his customers. This is a counter-surveillance technique intended to make it harder for law enforcement to identify the user of the phones and his associates.

17. Your Affiant also knows that traffickers commonly text message, each other or their customers, such as meeting locations, prices, and other information needed to carry out the sale of drugs (sometimes in code) and do so using cellular telephones and smart phones. In these communications, drug traffickers also discuss the price, quantity, and availability of narcotics as well as the distribution of narcotics. Drug traffickers also coordinate the shipment of narcotics from source locations to distribution locations. Drug traffickers also relay how to collect payment for the purchase of these narcotics.

18. Your affiant knows that traffickers, using digital cameras located on their cellular phone or other electronic devices, will sometimes use these devices to take photographs or videos of themselves, their location, their product, their firearms or their associates, which can be electronically stored on and transmitted from these electronic devices.

19. In my training and experience, I have learned that AT&T Wireless is a company that provides cellular telephone access to the general public, and that stored electronic communications, including retrieved and unretrieved voicemail, text, multimedia messages, phone location information, call detail records, and payment information for AT&T Wireless subscribers may be located on the computers of AT&T Wireless. Further, I am aware that computers located at AT&T Wireless contain information and other stored electronic communications belonging to unrelated third parties.

20. Wireless phone providers often provide their subscribers with voicemail services. In general, a provider will store voicemail messages on behalf of a particular subscriber until the subscriber deletes the voicemail. If the subscriber does not delete the message, the message may remain in the system of AT&T Wireless for weeks or months.

21. Among the services commonly offered by wireless phone providers is the capacity to send short text or multimedia messages (photos, audio, or video) from one subscriber's phone or wireless device to another phone or wireless device via one or more wireless providers. This service is often referred to as "Short Message Service" ("SMS") or "Multimedia Messaging Service" ("MMS"), and is often referred to generically as "text messaging." Based on my knowledge and experience, I believe that stored electronic communications, including SMS and MMS messages that have been sent or received by subscribers, may be stored by AT&T Wireless for short periods incident to and following their transmission. In addition, providers occasionally retain printouts from original storage of text messages for a particular subscriber's account.

22. Wireless phone providers typically retain certain transactional information about the use of each telephone, voicemail, and text-messaging account on their systems. This information can include log files and messaging logs showing all activity on the account, such as local and long distance telephone connection records, records of session times and durations, lists of all incoming and outgoing telephone numbers or e-mail addresses associated with particular telephone calls, voicemail messages, and text or multimedia messages. Providers may also have information about the dates, times, and methods of connecting associated with every communication in which a particular cellular device was involved.

23. Wireless providers may also retain text messaging logs that include specific information about text and multimedia messages sent or received from the account, such as the dates and times of the messages. A provider may also retain information about which cellular handset or device was associated with the account when the messages were sent or received. The provider could have this information because each cellular device has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular device could take several different forms, including an Electronic Serial Number ("ESN"), a Mobile Electronic Identity Number ("MEIN"), a Mobile Identification Number ("MIN"), a Subscriber Identity Module ("SIM"), an International Mobile Subscriber Identifier ("IMSI"), or an International Mobile Station Equipment Identity ("IMEI"). When a cellular device connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower in order to obtain service, and the cellular antenna or tower records those identifiers as a matter of course.

24. Many wireless providers retain information about the location in which a particular communication was transmitted or received. This information can include data about which "cell towers" (i.e., antenna towers covering specific geographic areas) received a radio signal from the cellular device and thereby transmitted or received the communication in question.

25. Wireless providers also maintain business records and subscriber information for particular accounts. This information could include the subscribers' full names and addresses, the address to which any equipment was shipped, the date on which the account was opened, the length of service, the types of service utilized, the ESN or other unique identifier for the cellular

device associated with the account, the subscribers' Social Security Numbers and dates of birth, all telephone numbers and other identifiers associated with the account, and a description of the services available to the account subscribers. In addition, wireless providers typically generate and retain billing records for each account, which may show all billable calls (including outgoing digits dialed). The providers may also have payment information for the account, including the dates, times and sometimes, places, of payments and the means and source of payment (including any credit card or bank account number).

26. In some cases, wireless subscribers may communicate directly with a wireless provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Wireless providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications.

27. As explained below, information stored at the wireless provider, including that described above, may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the data pertaining to a particular cellular device that is retained by a wireless provider can indicate who has used or controlled the cellular device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, data collected at the time of account sign-up, information relating to account payments, and communications (and the data associated with the

foregoing, such as date and time) may indicate who used or controlled a cellular device at a relevant time. Further, such stored electronic data can show how and when the cellular device and associated cellular service were accessed or used. Such "timeline" information allows investigators to understand the chronological context of cellular device usage, account access, and events relating to the crime under investigation. This "timeline" information may tend to either inculpate or exculpate the cellular device owner. Additionally, information stored by the wireless provider may indicate the geographic location of the cellular device and user at a particular time (e.g., historic cell-site location information; location integrated into an image or video sent via text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the state of mind of the cellular device's owner and/or user as it relates to the offense under investigation. For example, information relating to the cellular device in the possession of the wireless provider may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

28. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require AT&T Wireless to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

29. Based on the forgoing, I request that the Court issue the proposed search warrant.

30. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

31. The government will execute this warrant by serving the warrant on AT&T Wireless. Because the warrant will be served on AT&T Wireless, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

32. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee/continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

/Robert M. Buzzard

Robert Buzzard
Special Agent
FBI

Subscribed and sworn to before me on Jan 13, 2020

Sharon L Ovington

Hon. Sharon L. Ovington
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with (937) 238-1132 and (704) 497-3706 that is stored at premises owned, maintained, controlled, or operated by AT&T Wireless, a wireless provider headquartered at 11760 US Highway 1, Ste. 600, North Palm Beach, FL 33408.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by AT&T Wireless

To the extent that the information described in Attachment A is within the possession, custody, or control of **AT&T Wireless**, regardless of whether such information is located within or outside of the United States, and including any messages, records, files, logs, or information that have been deleted but are still available to **AT&T Wireless** or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), **AT&T Wireless** is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. Subscriber information, payment, call logs, call detail records including cell site information, sms text records including cell site information, data session records including cell site information, text message content, Per Call Measurement Data (PCMD) and/or RTT information, NELOS data, voice mails, and multimedia messages from January 2019 through November 5, 2019 stored and presently contained in, or on behalf of the account or identifier;

The Provider is hereby ordered to disclose the above information to the government within **fourteen days** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, evidence and instrumentalities of violations of 21 U.S.C. § 841(a)(1) (possession with intent to distribute controlled substances; 21 U.S.C. § 843(b) (use of a telephone communication facility to facilitate a drug trafficking crime); 21 U.S.C. § 846 (conspiracy to possess with intent to distribute

controlled substances); 21 U.S.C. § 856(maintaining a drug premises); and 18 U.S.C. § 924(c) (use and carrying of a firearm during and in relation to a drug trafficking crime) involving Nathan GODDARD, Cahke CORTNER, Lionel COMBS III, and Courtney Allen since January 2019 to November 5, 2019, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

a. List of customers and related identifying information;

b. Types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

c. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information);

d. Any information related to customers for drugs (including names, addresses, phone numbers, or any other identifying information);

e. Any information identifying other individuals who participate in the sale, distribution or acquisition of drugs with Nathan GODDARD, Cahke CORTNER, Lionel COMBS III, and Courtney ALLEN;

f. Information relating to the use, possession, or acquisition of firearms, ammunition, or other weapons;

g. Information relating to the use or threatened use of violence in connection with the drug trade;

h. Information relating to bulk cash, jewelry, automobile or other common proceeds of the drug trade;

i. Any information recording schedules or travel from January 2019 to the present;

j. All bank records, checks, credit card bills, account information, and other financial records.

k. Evidence indicating how and when the cellular device and associated cellular service was used to determine the chronological context of cellular device use, account access, and events relating to the crime under investigation;

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT C

Code Section	*Offense Description*
21 U.S.C. § 841(a)(1)	Possession with intent to distribute controlled substances
21 U.S.C. § 843(b)	Use of a telephone communication facility to facilitate a drug trafficking crime
21 U.S.C. § 846	Conspiracy to possess with intent to distribute controlled substances
21 U.S.C. § 856	Maintaining a drug premises
18 U.S.C. § 924(c)	Use and carrying of a firearm during and in relation to a drug trafficking crime